IV. REMARKS

1.   The specification, drawings and claims 1, 9, 11, 13, 19, 21, 22, 24, 28, 32, 38, 50, 57, 58, 60, 64 and 67 have been amended. Claims 1 through 72 are now pending in this application.

2.   The references to the "Information Based Indicia Program (IBIP) Open System Indicium Specification," dated August 19, 1998 and "Digital Signature Standard (DSS)" FIPS PUB 186, May 19, 1994 cited in the specification are not currently in Applicant's possession. Efforts will we made to obtain these references and upon receipt these references will be forwarded to the Examiner.

3.   The specification has been amended with respect to Applicant's claim for priority under 35 U.S.C. 199(e)/120.

4.   A copy of the Abstract on a separate sheet is being provided herewith as requested by the Examiner. It is noted however that M.P.E.P. § 1893.03(e) states that "it is improper for the Examiner of the U.S. national stage application to require the applicant to provide an abstract commencing on a separate sheet if the abstract does not appear on a separate sheet in the pamphlet."

5.   The drawings are amended to address the objections noted by the Examiner. The specification has also been amended to overcome the objections. Figure 3 is amended to show a "counter" and corresponding language has been added to the specification regarding the same. A corresponding drawing replacement sheet is appended.

6.   The claims are amended to overcome the rejection under 35 U.S.C. 112, second paragraph. The amendments to the claims in response to the 35 U.S.C. 112 rejection do not limit or narrow these claims.

7.   The claims are amended to overcome the rejection under 35 U.S.C. 101. The amendments to the claims in response to the 35 U.S.C. 101 rejection do not limit or narrow these claims.

8.   Claims 1-31 and 38-66 were rejected under 35 U.S.C. 103(a) as being unpatentable over either Haines et al., U.S. Patent 5,077,660 or 5,107,455 in view of Obrea, U.S. Patent 4,785,417 and Hall, U.S. Publication T104,003. The Applicant respectfully disagrees. Claim 1 of the present application, as amended, recites in pertinent part, a processing unit, operatively connected to the memory and the device for receiving an authorization code, for verifying at least part of the authorization code to detect any unauthorized change in the software component before the at least one postage indicium is generated, the detection of any unauthorized change preventing generation of the at least one postage indicium.

Claim 38 of the present application recites in pertinent part, verifying at least part of the authorization code to detect any unauthorized change in the software component before the at least one postage indicium is generated, the detection of any unauthorized change preventing generation of the at least one postage indicium.

Haines et al., ('660) discloses a technique for reconfiguring, in the field, a postage meter having a set of features that can be selectively enabled or disabled by software. Haines '660 teaches

a way to manufacture a generic meter, that once delivered to a customer can become activated, by interaction with a data center, to operational parameters/features associated with a particular customer. For example, the meter can print five numerical postage value digits, but the specific installation is associated with only printing four postage value digits. So although the software is capable of printing 5 postal digits, the small customer can acquire a less expensive meter with only four physically printing digits. Upon the first data center call-in, thee software is set to program only a four-digit machine operation.

In Haines '660 a configuration enable code is used for reconfiguring the meter (col. 4, l. 53-61). An agent receives the enable code and enters it into the meter. The meter then generates its own enable code and if that meter generated code matches the enable code input by the agent the meter is reconfigured (col. 7 l. 15-58). The enable code in Haines '660 is generated by an encryption routine performed on a configuration transaction identifier (CTID), which is dependent on the meter serial number, as the key and a combination of the old and new meter type number (MTN), representing the set of features enabled as the input number. Haines '660 also discloses the input number as a combination of the meter serial number and high security length (HSL) value as the input number (col. 10, l. 10-39).

Haines et al., ('455) discloses a technique for reconfiguring, in the field, external devices in communication with a postage meter. Haines '455 is concerned with configuring devices connected to a meter (especially a scale) where the devices themselves cannot communicate with an external data center to

receive configuration instructions. The meter is used to convey (scale) configuration information as provided by the meter data center.

In Haines '455, an agent receives the enable code and enters it into the meter. The meter then generates its own enable code and if that meter generated code matches the enable code input by the agent the meter is reconfigured (col. 6 l. 32-51). The enable code in Haines '455 is generated by an encryption routine performed on the CTID as the key and a combination of the meter serial number, status code and HSL value or a combination of the ascending register amount, meter serial number, and status code as the input number (col. 7 l. 4-12).

Nowhere in Haines (either '660 or '455) is the verification of at least part of the authorization code to detect any unauthorized change in the software component, as claimed by Applicant, disclosed or suggested.

Obrea discloses a postage meter including a method for checking the particular operation being carried out by the meter is being carried out in the appropriate sequence under the given conditions. The purpose of Obrea is to ensure that a program step counter does not get mis-synchronized to accidentally run code not planned to be run at any given time. A code word can be placed as many times as wished in any routine and checked during the running of the routine. If the code word was always the same (for the specific routine running), then everything is OK. In Obrea, an expected password is stored in RAM (see Fig. 2A). Password checks are inserted into the program steps of the running program. The program takes the RAM password and compares it with a password in read only memory and if the comparison is true the program returns to its normal operation (col. 3 l. 46-

63).   For example, if the program glitches and the program counter is reset and suddenly code is being executed that should not be running, the incorrect code word shows up and the meter can be stopped.

This is not what is being claimed in Claim 1 of the present application.

Nowhere in Obrea is the verification of an authorization code to detect any unauthorized change in the software component disclosed or suggested. Rather, in Obrea the password is used to check if a program is running out of sequence and not for verifying that no unauthorized changes have been made to that program.   Claims 1 and 38 of the present application recite verifying at least part of the authorization code to detect any unauthorized change in the software component.   Since neither Haines '455, Haines '660 nor Obrea disclose or suggest at least this feature, their combination cannot as well.

Hall et al. discloses the use of a CRC quantity for a frame check sequence (see Fig. 1).   Nowhere in Hall is it disclosed or suggested to verify an authorization code to detect any unauthorized change in the software component as claimed in the present application.   Thus, the combination of Haines '455, Haines '660, Obrea and Hall cannot as well.

It is submitted that there is no motivation or suggestion to combine the cited references to achieve Applicant's results in Claims 1 and 38 of the present application. If Haines ('660 and '455), Obrea and Hall were combined the result would be a postage meter having a program with a cyclic redundancy check to verify that the program was running in sequence.   This is not what is being claimed in Claims 1 and 38 of the present application.

Claims 1 and 38 of the present application recite verifying at least part of the authorization code to detect any <u>unauthorized change</u> in the <u>software component</u> before the at least one postage indicium is generated. Accordingly, Claim 1 of the present application is not obvious over Haines ('660 and '455), Obrea and Hall and is patentable under 35 U.S.C. 103(a).

Claims 2-12 depend from independent Claim 1 and Claims 39-49 depend from Claim 38 and should also be allowable at least because of their respective dependencies.

Claim 13 of the present application recites in pertinent part, a buffer, operably connected to the memory, for storing an authorization code which is derived from at least information concerning a configuration of the system. Claim 13 also recites, a processing unit, operatively connected to the memory and buffer, for verifying at least part of the authorization code before the at least one postage indicium is generated to detect any unauthorized change in the configuration of the franking system, the detection of any unauthorized change by the processing unit preventing generation of the at least one postage indicium by the software component.

Claim 50 of the present application recites in pertinent part, storing an authorization code which is derived from at least information concerning a configuration of the system. Claim 50 also recites verifying at least part of the authorization code before the at least one postage indicium is generated to detect any unauthorized change in the configuration of the franking system, the detection of any unauthorized change by the processing unit preventing generation of the at least one postage indicium by the software component.

Haines ('660) discloses an enable code generated by an encryption routine performed on a configuration transaction identifier (CTID), which is dependent on the meter serial number, as the key and a combination of the old and new meter type number (MTN), representing the set of features enabled as the input number. Haines ('660) also discloses the input number as a combination of the meter serial number and high security length (HSL) value as the input number (col. 10 1. 10-39). Although Haines ('660) discloses an enable code dependent on the set of features enabled in the meter, Haines ('660) does not disclose verifying the enable code to check for unauthorized changes to the configuration of that meter.

Haines ('455) discloses an enable code generated by an encryption routine performed on the CTID as the key and a combination of the meter serial number, status code and HSL value or a combination of the ascending register amount, meter serial number, and status code as the input number. Nowhere in Haines ('455) is it suggested or disclosed that the enable code is derived from information concerning a configuration of the system nor is it disclosed to verify the enable code to check for unauthorized changes to the configuration of the meter. Since neither Haines ('660) nor Haines ('455) disclose at least this feature their combination cannot as well.

In Haines ('660 and '455) the enable code is verified by the meter so that an authorized change in meter configuration can be made. In Haines ('660 and '455), only an agent can reconfigure the postage meter by pressing a certain key sequence and entering a service access code known only by the agent ('660 at col. 4 1. 43-45 and col. 5 1. 1-12; '455 at col. 4 1. 39-50). The enable code in Haines ('660 and '455) is verified by the meter to ensure

the agent configured the meter properly, not to detect any unauthorized change in the configuration of the franking system. This is contrary to what is being claimed in claims 13 and 50 of the present application.

Claims 13 and 50 of the present application recite verifying at least part of the authorization code before the at least one postage indicium is generated to detect any unauthorized change in the configuration of the franking system.

Obrea discloses a postage meter including a method for checking the particular operation being carried out by the meter is being carried out in the appropriate sequence under the given conditions. There is no disclosure or suggestion of detecting any unauthorized change in the configuration of the franking system in Obrea. Neither Haines ('660 and '455) nor Obrea disclose or suggest at least this feature, thus their combination cannot as well.

Likewise, Hall does not disclose or suggest detecting any unauthorized change in the configuration of the franking system. Therefore, the combination of Haines ('660 and '455), Obrea and Hall cannot disclose or suggest this feature either.

If Haines ('660 and '455) were combined with Obrea and Hall the result would be a postage meter having a program with a cyclic redundancy check to verify that the program was running in sequence and the verification of an authorized change in the meter configuration. This is not what is claimed in Claims 13 and 50 of the present application. Claims 13 and 50 recite verifying at least part of the authorization code before the at least one postage indicium is generated to detect any unauthorized change in the configuration of the franking system

made by the user. Claims 13 and 50 are patentable under 35 U.S.C. 103(a).

Claims 14-20 depend from Claim 13 and Claims 51-56 depend from Claim 50 and should also be allowable at least because of their respective dependencies.

Claim 21 of the present application recites in pertinent part, the authorization code comprising a code segment and a data segment. The code segment being derived from at least information concerning the selected setting of the feature options, the data segment containing data concerning one or more of the feature options.

Claim 57 of the present application recites in pertinent part, the authorization code comprising a code segment and a data segment, the code segment being derived from at least information concerning the selected setting of the feature options, the data segment containing data concerning one or more of the feature options.

Neither Haines ('660) nor Haines ('455) disclose or suggest a code segment being derived from at least information concerning the selected setting of the feature options. Nor does Haines ('660) or Haines ('455) disclose or suggest the data segment containing data concerning one or more of the feature options. As such, the combination of Haines ('660) and Haines ('455) cannot suggest or disclose these features as well.

Haines ('660) discloses an enable code generated by an encryption routine performed on a configuration transaction identifier (CTID), which is dependent on the meter serial number, as the key (or code segment) and a combination of the old and new meter type number (MTN), representing the set of features enabled as the

28

input number (or data segment). Haines ('660) also discloses the input number as a combination of the meter serial number and high security length (HSL) value (col. 10 l. 10-39). This is contrary to what is claimed in Claims 21 and 57 of the present application.

In claims 21 and 57 the code segment is derived from at least information concerning the selected setting of the feature options whereas in Haines ('660) the key or code segment is derived from the configuration transaction identifier (CTID). The CTID in Haines ('660) is dependent on the meter serial number (col. 10 l. 10-39). There is no suggestion or disclosure in Haines ('660) that the key segment of the enable code is derived from the meter configuration.

Likewise in Haines ('455) the enable code is generated by an encryption routine performed on the CTID as the key (or code segment) and a combination of the meter serial number, status code and HSL value as the input number (or data segment). Haines ('455) also discloses the input number as a combination of the ascending register amount, meter serial number, and status code (col. 7 l. 4-12). Again there is no suggestion or disclosure in Haines ('455) that the key segment of the enable code is derived from the meter configuration. As such, the combination of Haines ('660) and Haines ('455) cannot disclose or suggest this feature either.

Claims 21 and 57 of the present application recite the code segment being derived from at least information concerning the selected setting of the feature options. There is no motivation or suggestion to combine Haines ('660) and Haines ('455) to achieve the results obtained by the Applicant in the present application. If Haines ('660) and Haines ('455) where combined

29

you would have an enable code with a key generated from the CTID and an input number made of a combination of the old and new MTN, the HSL value, the meter serial number, the status code and ascending register amount. Accordingly, Claims 21 and 57 are patentable under 35 U.S.C. 103(a).

Claims 22-27 depend from Claim 21 and Claims 58-63 depend from Claim 57 and should also be allowable at least because of their respective dependencies.

Claim 28 of the present application recites in pertinent part, a first memory for storing a first software component for generating at least one postage indicium. Claim 28 also recites, a second software component being stored in the first memory for interacting with the first software component, the second software component including a selected identifier.

Claim 64 of the present application recites in pertinent part, storing a first software component in a first memory for generating at least one postage indicium. Claim 64 also recites, storing a second software component in a first memory for interacting with the first software component, the second software component including a selected identifier.

Haines ('660) discloses a meter with a set of features that may be selectively enabled or disabled by software. Haines '660 also discloses the meter having software for generating an encrypted configuration request code. Nowhere in Haines '660 is it suggested or disclosed that the meter has two interacting software components stored in the same memory.

Likewise, Haines ('455) discloses meter software that generates

an encrypted I/O configuration request code but fails to suggest or disclose a meter having two interacting software components stored in the same memory.

In Haines (both '660 and '455) the software in the meter and the software in the data center computer interact. However the software in the meter and the software in the data center computer cannot be stored in the same memory as the meter is in a remote location from the data center computer. As such, if Haines ('660) were combined with Haines ('455) you would have a meter with software for interacting with software in the data center computer. This is not what is being claimed in Claims 28 and 64 of the present application.

Claim 28 recites a first software component in a first memory for realizing at least one postage indicium and a second software component in a first memory for interacting with the first software component. Claim 64 recites a first software component in a first memory for realizing at least one postage indicium and a second software component in a first memory for interacting with the first software component. Claims 28 and 64 are patentable under 35 U.S.C. 103(a).

Claims 29-31 depend from Claim 28 and Claims 65-66 depend from Claim 64 and should also be allowable at least because of their respective dependencies.

9. Claims 32-37 and 67-72 were rejected under 35 U.S.C. 103(a) as being unpatentable over either Haines et al., U.S. Patent 5,077,660 or 5,107,455 in view of Obrea, U.S. Patent 4,785,417, Hall, U.S. Publication T104,003 and Smith et al., U.S. Patent 6,067,582. The Applicant respectfully disagrees. Claim 32 of

the present application recites in pertinent part, a memory for storing a value of an account for replenishing the postage fund in the franking apparatus. Claim 32 also recites, a processor, operably connected to the memory, for reconfiguring the franking apparatus, a reconfiguration of the franking apparatus incurring a cost, the cost being separate from the postage fund, the value of the account being adjusted to account for the cost, the value of the postage fund in the franking apparatus being unaffected by the reconfiguration.

Claim 67 of the present application recites in pertinent part, storing a value of an account for replenishing the postage fund in the franking apparatus. Claim 67 also recites, reconfiguring the franking apparatus, a reconfiguration of the franking apparatus incurring a cost, the cost being separate from the postage fund, and adjusting the value of the account to account for the cost, the value of the postage fund in the franking apparatus being unaffected by the reconfiguration.

Neither Haines ('660 and '455), Hall nor Obrea disclose or suggest the reconfiguring of the franking apparatus incurring a cost, the cost being separate from the postage fund. Nor do they disclose or suggest adjusting the value of the account to account for the cost, the value of the postage fund in the franking apparatus being unaffected by the reconfiguration. Likewise, Smith does not disclose the reconfiguration of a franking machine or how the funds within that franking machine are affected by such a reconfiguration. Accordingly, the combination of Haines ('660 and '455), Hall, Obrea and Smith cannot disclose these features as well.

Smith et al., discloses a method for controlling software

32

distribution over a network by embedding a sub-component of the distribution control software in each software application and having a central monitoring software for monitoring the distribution of software applications. Smith also discloses the user of the remote computer accepting the pricing of the software. The billing information or payment methods disclosed in Smith can be credit card numbers, debit card numbers, a pre-established account number, or a bank account number. However, Smith does not disclose or suggest the reconfiguration of a franking machine or how the funds within the franking machine are affected from the purchase of a remote configuration change of the franking machine. Smith is directed to downloading purchased software and a connection between a server and an agent (client). There is noting in Smith about modifying or running with existing secure software or the use of "fail safe" encryption techniques to assure the requesting agent/client is actually allowed to request software. In Applicant's invention, the meter is already capable of running all the features and functions available to it. Applicant's methodology selects those features and functions allowed to be run based on a specific customer installation and services paid for.

The examiner acknowledges that Haines ('660 or '455) as modified by Obrea in view of Hall does not disclose or suggest billing the user of the franking machine for the reconfiguration of the system. As such, if Haines ('660 or '455) as modified in view of Hall were combined with Smith the reconfiguration of a postage meter over a network would result with payment for that reconfiguration taken from a credit card, debit card, a pre-established account number, or a bank account number. There is no motivation or suggestion to combine the cited references to achieve what is claimed by the Applicant in Claims 32 and 67.

33

Even when the suggested references are combined there remains no suggestion or disclosure of how the funds within the franking machine are affected by the reconfiguration of the franking machine.
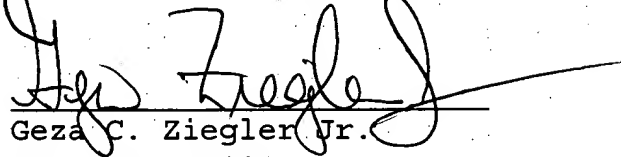
Claim 32 of the present application recites, a reconfiguration of the franking apparatus incurring a cost, the value of the account being adjusted to account for the cost, the value of the postage fund in the franking apparatus being unaffected by the reconfiguration. Claim 67 of the present application recites, a reconfiguration of the franking apparatus incurring a cost and adjusting the value of the account to account for the cost, the value of the postage fund in the franking apparatus being unaffected by the reconfiguration. Claims 32 and 67 are patentable under 35 U.S.C. 103(a).

Claims 33-37 depend from Claim 32 and Claims 68-72 depend from Claim 67 and should also be allowable at least because of their respective dependencies.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,

Geza C. Ziegler Jr.
Geza C. Ziegler Jr.
Reg. No. 44004

2 JUNE 2005
Date

Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date indicated below as first class mail in an envelope addressed to the Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: June 2, 2005   Signature: _Meaghan Baye_
                                     Person Making Deposit